

PCT/JP2004/000619

23. 1. 2004

#2

日本国特許庁  
JAPAN PATENT OFFICE

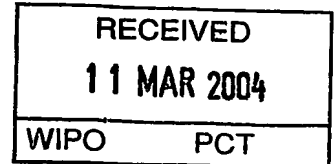
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application: 2003年 1月23日

出願番号  
Application Number: 特願2003-015233  
[ST. 10/C]: [J.P.2003-015233]

出願人  
Applicant(s): キヤノン株式会社

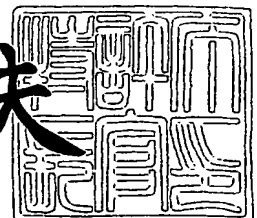


PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 2月26日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



出証番号 出証特2004-3013647

【書類名】 特許願

【整理番号】 251739

【提出日】 平成15年 1月23日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 7/00

【発明の名称】 情報処理方法

【請求項の数】 1

【発明者】

    【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号 キヤノン株式会社  
社内

    【氏名】 林 淳一

【発明者】

    【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号 キヤノン株式会社  
社内

    【氏名】 須賀 祐治

【特許出願人】

    【識別番号】 000001007

    【氏名又は名称】 キヤノン株式会社

【代理人】

    【識別番号】 100076428

    【弁理士】

    【氏名又は名称】 大塚 康德

【選任した代理人】

    【識別番号】 100112508

    【弁理士】

    【氏名又は名称】 高柳 司郎

【選任した代理人】

【識別番号】 100115071

【弁理士】

【氏名又は名称】 大塚 康弘

【選任した代理人】

【識別番号】 100116894

【弁理士】

【氏名又は名称】 木村 秀二

【手数料の表示】

【予納台帳番号】 003458

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0102485

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理方法

【特許請求の範囲】

【請求項 1】 符号化画像データを暗号化する情報処理方法であって、  
符号化画像データを入力する工程と、  
入力した符号化画像データを暗号化する工程と、  
符号化データのヘッダ部中の誤り検出符号有無を示す有無情報を、誤り検出符号無しに変更し、暗号化した符号化画像データを出力する工程と  
を備えることを特徴とする情報処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル画像データの圧縮符号化したデータを暗号化する技術に関するものである。

【0002】

【従来の技術】

従来、画像データなどを秘匿して伝送するために、画像データ全体の暗号化やスクランブルなどが行なわれてきた。これは、予め画像データ全体、或いはその一部を暗号鍵を用いて暗号化し、前記暗号鍵に対応する復号鍵を有するものだけが正しく復号することが可能であるようにする技術である。

【0003】

一方、画像データは情報量が大きい為に、これを効率的に伝送、及び蓄積する際に圧縮符号化を行う場合が多い。圧縮符号化としては、例えば ISO/IEC JTC 1/SC 29/WG1 にて標準化されている JPEG 2000 と呼ばれる技術などが有望視されている。従って、前述した画像データの暗号化は JPEG 2000 のような圧縮符号化された画像データに対して施されることが望まれる。

【0004】

JPEG 2000 においては、たとえ伝送過程で誤りが生じた場合でも、その

誤りを検知する機能を適応することが可能である。送信側で、この機能を用いて画像データを圧縮符号化して送信することによって、受信側で圧縮復号の際に誤りを検知した場合でも、誤っている部分のデータだけを再送するように送信側に再送要求を出し、再送されたデータを圧縮復号することによって、正しく復号可能となる。

#### 【0005】

##### 【発明が解決しようとする課題】

しかしながら、前述したように、誤り検出可能なように画像データを圧縮符号化し、更に、この圧縮符号化された画像データに対して暗号化処理を施した場合、誤り検知機能が正しく動作しない場合がある。これは、受信側において、暗号化された画像データを、（誤って）誤りが生じた画像データであると判定するからである。この場合、誤っていると判定された部分の再送要求を送信側にしたとしても、送信側から送られてくるのは当然のことながら（誤っていると判断された部分と）同じ画像データであり、場合によっては繰り返し再送要求をし続けることにもなりかねない。

#### 【0006】

本発明はかかる問題点に鑑みなされたものであり、誤り検出符号が付加された圧縮符号化画像データを暗号化したとしても、それを受信し再生する側の装置において無意味な再送要求等を行わず、正常な処理を行えるようにする技術を提供しようとするものである。

#### 【0007】

##### 【課題を解決するための手段】

この課題を解決するため、例えば本発明の情報処理方法は以下のような工程を備える。すなわち、

符号化画像データを暗号化する情報処理方法であって、

符号化画像データを入力する工程と、

入力した符号化画像データを暗号化する工程と、

符号化データのヘッダ部中の誤り検出符号有無を示す有無情報を、誤り検出符号無しに変更し、暗号化した符号化画像データを出力する工程とを備える。

## 【0008】

## 【発明の実施の形態】

以下、添付図面に従って本発明に係る実施形態を説明する。

## 【0009】

## &lt;全体構成の説明&gt;

実施形態におけるシステム概要例を図9に示す。図中、90はインターネットであって、91は例えばデジタルカメラやイメージスキャナ、フィルムスキャナ等で撮像した画像データを圧縮符号化&暗号化処理を行う装置である。92は画像データを受信し、復号する装置、93は復号する際に必要となる暗号化解除鍵を記憶している認証サーバある。装置91乃至93はパーソナルコンピュータ等の汎用装置で構わない。処理の流れを簡単に説明すると、次の通りである。

## 【0010】

装置91では、所望とする画像データを圧縮符号化及び暗号化処理を行い、インターネット90を介して配布する。配布するのは装置91が直接行ってもよいし、適当なサーバを介して配布しても構わない。ただし、暗号化されている関係で、その解除するために必要な鍵情報を、その画像データを特定する情報（例えばID）と共に認証サーバ93が有するDBに登録しておく。画像復号装置92は所望とする画像を受信し、復号を行ない閲覧するものであるが、暗号化されている画像データを閲覧するには、認証サーバ93にその画像を特定する情報を通知して、暗号化解除鍵情報を要求する。この結果、暗号化解除鍵情報が認証サーバ93より受信するので、それを用いて暗号化を解除し、復号再生する。

## 【0011】

## &lt;圧縮符号化処理部&gt;

まずはじめに、図1を用いて、画像データ圧縮&暗号化装置91における圧縮符号化処理、及びその過程で実行される誤り検出符号化機能を説明する。

## 【0012】

図1において、11は画像入力部、12は離散ウェーブレット変換部、13は量子化部、14はエントロピ符号化部、15は符号出力部である。まず、画像入力部11に対して符号化対象となる画像を構成する画素信号がラスタースキャン

順に入力され、その出力は離散ウェーブレット変換部 12 に入力される。以降の説明では画像信号はモノクロの多値画像を表現しているが、カラー画像等、複数の色成分を符号化するならば、RGB 各色成分、或いは輝度、色度成分を上記単色成分として圧縮すればよい。

### 【0013】

離散ウェーブレット変換部 12 は、入力した画像信号に対して 2 次元の離散ウェーブレット変換処理を行い、変換係数を計算して出力するものである。図 2 (a) は離散ウェーブレット変換部 12 の基本構成を表したものであり、入力された画像信号はメモリ 21 に記憶され、処理部 22 により順次読み出されて変換処理が行われ、再びメモリ 21 に書きこまれており、本実施の形態においては、処理部 22 における処理の構成は同図 (b) に示すものとする。同図において、入力された画像信号は遅延素子およびダウンサンプラの組み合わせにより、偶数アドレスおよび奇数アドレスの信号に分離される。すなわち、入力される画素データは、ここで偶数番目の画素と奇数番目の画素に分けられることになる。分離された夫々の画素データは、2 つのフィルタ p および u によりフィルタ処理が施される。同図 s および d は、各々 1 次元の画像信号に対して 1 レベルの分解を行った際のローパス係数およびハイパス係数を表しており、次式により計算されるものとする。

$$d(n) = x(2*n+1) - \text{floor}((x(2*n) + x(2*n+2))/2) \quad (\text{式 1})$$

$$s(n) = x(2*n) + \text{floor}((d(n-1) + d(n))/4) \quad (\text{式 2})$$

ただし、 $x(n)$  は変換対象となる画像信号である。

### 【0014】

以上の処理により、画像信号に対する 1 次元の離散ウェーブレット変換処理が行われる。2 次元の離散ウェーブレット変換は、1 次元の変換を画像の水平・垂直方向に対して順次行うものであり、その詳細は公知であるのでここでは説明を省略する。図 2 (c) は 2 次元の変換処理により得られる 2 レベル (ウェーブレット変換回数が「2」という意味) の変換係数群の構成例であり、画像信号は異なる周波数帯域の係数列 HH1、HL1、LH1、…、LL に分解される。なお、以降の説明ではこれらの係数列をサブバンドと呼ぶ。各サブバンドの係数は後

続の量子化部 13 に出力される。

#### 【0015】

量子化部 13 は、入力した係数を所定の量子化ステップにより量子化し、その量子化値に対するインデックスを出力する。ここで、量子化は次式により行われる。

$$q = \text{sign}(c) \text{ floor}(\text{abs}(c) / \Delta) \quad (\text{式 3})$$

$$\text{sign}(c) = 1; c \geq 0 \quad (\text{式 4})$$

$$\text{sign}(c) = -1; c < 0 \quad (\text{式 5})$$

ここで、 $c$  は量子化対象となる係数である。また、本実施の形態においては  $\Delta$  の値として 1 を含むものとする。この場合実際に量子化は行われず、量子化部 13 に入力された変換係数はそのまま後続のエントロピ符号化部 14 に出力される。

#### 【0016】

エントロピ符号化部 14 は入力した量子化インデックスをビットプレーンに分解し、ビットプレーンを単位に 2 値算術符号化を行ってコードストリームを出力する。図 3 はエントロピ符号化部 14 の動作を説明する図であり、この例においては  $4 \times 4$  の大きさを持つサブバンド内の領域において非 0 の量子化インデックスが 3 個存在しており、それぞれ +13、-6、+3 の値を持っている。エントロピ符号化部 14 はこの領域を走査して最大値  $M$  を求め、次式により最大の量子化インデックスを表現するために必要なビット数  $S$  を計算する。

$$S = \text{ceil}(\log_2(\text{abs}(M))) \quad (\text{式 8})$$

ここで  $\text{ceil}(x)$  は  $x$  以上の整数の中で最も小さい整数値を表す。

#### 【0017】

図 3 においては、最大の係数値は 13 であるので  $S$  は 4 であり、シーケンス中の 16 個の量子化インデックスは同図 (b) に示すように 4 つのビットプレーンを単位として処理が行われる。最初にエントロピ符号化部 14 は最上位ビットプレーン (同図 MSB で表す) の各ビットをエントロピ符号化 (本実施の形態では 2 値算術符号化) し、ビットストリームとして出力する。次にビットプレーンを 1 レベル下げ、以下同様に対象ビットプレーンが最下位ビットプレーン (同図 LS

Bで表す)に至るまで、ビットプレーン内の各ビットを符号化し符号出力部15に出力する。なお上記エントロピ符号化時において、各量子化インデックスの符号は、上位から下位へのビットプレーン走査において最初(最上位)に符号化されるべき非0ビットが検出されるとそのすぐ後に当該量子化インデックスの正負符号を示す1ビットを続けて2値算術符号化することとする。これにより、0以外の量子化インデックスの正負符号は効率良く符号化される。

#### 【0018】

ここで、本実施形態における誤り検出符号化について図10を用いて説明する。図10において、101は前述した一つのビットプレーン内の各ビットの並びである。また、102は誤り検出符号化のために101の後に添付される所定の情報である。以降では、この所定の情報をセグメンテーションシンボルと呼ぶ。本実施形態における誤り検出符号化は、図10に示すように、本来エントロピ符号化される情報(101)の後にセグメンテーションシンボル(102)を添付した情報全体をエントロピ符号化するようにして実行する。尚、前記セグメンテーションシンボルは、圧縮符号化処理部と後述する圧縮復号処理部において同じ値を用いるようにする。

#### 【0019】

図4は、このようにして生成され出力される符号列の構成を表した概略図である。同図(a)は符号列の全体の構成を示したものであり、MHはメインヘッダ、THはタイルヘッダ、BSはビットストリームである。メインヘッダMHは同図(b)に示すように、符号化対象となる画像のサイズ(水平および垂直方向の画素数)、画像を複数の矩形領域であるタイルに分割した際のサイズ、各色成分数を表すコンポーネント数、各成分の大きさ、ビット精度を表すコンポーネント情報から構成されている。なお、本実施の形態では画像はタイルに分割されていないので、タイルサイズと画像サイズは同じ値を取り、対象画像がモノクロの多値画像の場合コンポーネント数は1である。

#### 【0020】

次にタイルヘッダTHの構成を図4(c)に示す。タイルヘッダTHには当該タイルのビットストリーム長とヘッダ長を含めたタイル長および当該タイルに対

する符号化パラメータから構成される。符号化パラメータには離散ウェーブレット変換のレベル、フィルタの種別等が含まれている。更に、前述した誤り検出符号化が適用されているか否かを示す情報も、この符号化パラメータに含まれている。以降では、この誤り検出符号化が適用されているか否かを示す情報（1ビットで良い）を「第1の誤り検出符号化情報」と呼ぶ。そして、第1の誤り検出符号化情報が“0”の時には誤り検出符号化はされていないことを示し、一方で第1の誤り検出符号化情報が“1”の場合には誤り検出符号化されていることを示すことにする。

#### 【0021】

本実施の形態におけるビットストリームの構成を同図（d）に示す。同図において、ビットストリームは各サブバンド毎にまとめられ、解像度の小さいサブバンドを先頭として順次解像度が高くなる順番に配置されている。さらに、各サブバンド内は上位ビットプレーンから下位ビットプレーンに向かい、ビットプレーンを単位として符号が配列されている。

#### 【0022】

上記符号配列とすることにより、後述する図8の様な階層的復号化を行うことが可能となる。

#### 【0023】

上述した実施の形態において、符号化対象となる画像全体の圧縮率は量子化ステップ $\Delta$ を変更することにより制御することが可能である。

#### 【0024】

また別の方法として本実施の形態では、エントロピ符号化部14において符号化するビットプレーンの下位ビットを必要な圧縮率に応じて制限（廃棄）することも可能である。この場合には、全てのビットプレーンは符号化されず上位ビットプレーンから所望の圧縮率に応じた数のビットプレーンまでが符号化され、最終的な符号列に含まれる。

#### 【0025】

##### <圧縮復号処理部>

次に以上述べた圧縮符号化処理部による符号列を復号する方法、及び誤り検出

機能について説明する。図5は本実施の形態における圧縮復号化処理部の構成を表すブロック図であり、51が符号入力部、52はエントロピ復号部、53は逆量子化部、54は逆離散ウェーブレット変換部、55は画像出力部である。

#### 【0026】

符号入力部51は符号列を入力し、それに含まれるヘッダを解析して後続の処理に必要なパラメータを抽出し必要な場合は処理の流れを制御し、あるいは後続の処理ユニットに対して該当するパラメータを送出するものである。また、符号列に含まれるビットストリームはエントロピ復号部52に出力される。

#### 【0027】

エントロピ復号部52はビットストリームをビットプレーン単位で復号し、出力する。この時の復号化手順を図6に示す。図6(a)は復号対象となるサブバンドの一領域をビットプレーン単位で順次復号化(4プレーン時の場合)し、最終的に量子化インデックスを復元する流れを図示したものであり、同図の矢印の順にビットプレーンが復号される。復元された量子化インデックスは逆量子化部53に出力される。

#### 【0028】

ここで、本実施形態における誤り検出機能について説明する。誤り検出符号化されているか否かは、入力された符号列中に含まれるヘッダを解析し、ヘッダ中の符号化パラメータに含まれる第1の誤り検出符号化情報により判定可能である。第1の誤り検出符号化情報が“1”の場合(誤り検出符号化されていると判定された場合)には、エントロピ復号された後のビットプレーンのうち、添付されたセグメンテーションシンボル(図10における102)が、前述した符号化処理部において添付したセグメンテーションシンボルと一致するか否かを調べる。一致する場合には、誤りは生じていないと判定でき、一致しない場合には誤りが生じていると判定できる。誤りが生じている場合には、該ビットプレーンを送信側に再送するようにすれば正しく圧縮復号可能となる。

#### 【0029】

次に、逆量子化部53は入力した量子化インデックスから、次式に基づいて離散ウェーブレット変換係数を復元する。

$$c' = \Delta * q; \quad q \neq 0 \quad (\text{式 9})$$

$$c' = 0 \quad ; \quad q = 0 \quad (\text{式 10})$$

ここで、 $q$  は量子化インデックス、 $\Delta$  は量子化ステップであり、 $\Delta$  は符号化時に用いられたものと同じ値である。 $c'$  は復元された変換係数であり、符号化時では  $s$  または  $d$  で表される係数の復元したものである。変換係数  $c'$  は後続の逆離散ウェーブレット変換部 54 に出力される。

### 【0030】

図 7 は逆離散ウェーブレット変換部 54 の構成および処理のブロック図を示したものである。同図 (a) において、入力された変換係数はメモリ 71 に記憶される。処理部 72 は 1 次元の逆離散ウェーブレット変換を行い、メモリ 71 から順次変換係数を読み出して処理を行うことで、2 次元の逆離散ウェーブレット変換を実行する。2 次元の逆離散ウェーブレット変換は、順変換と逆の手順により実行されるが、詳細は公知であるので説明を省略する。また同図 (b) は処理部 72 処理ブロックを示したものであり、入力された変換係数は  $u$  および  $p$  の 2 つのフィルタ処理を施され、アップサンプリングされた後に重ね合わされて画像信号  $x'$  が出力される。これらの処理は次式により行われる。

$$x'(2*n) = s'(n) - \text{floor}((d'(n-1) + d'(n))/4) \quad (\text{式 15})$$

$$x'(2*n+1) = d'(n) + \text{floor}((x'(2*n) + x'(2*n+2))/2) \quad (\text{式 16})$$

ここで、(式 1)、(式 2)、および (式 15)、(式 16) による順方向および逆方向の離散ウェーブレット変換は完全再構成条件を満たしているため、本実施形態において量子化ステップ  $\Delta$  が 1 であり、ビットプレーン復号において全てのビットプレーンが復号されていれば、復元された画像信号  $x'$  は原画像の信号  $x$  と一致する。

### 【0031】

以上の処理により画像が復元されて画像出力部 55 に出力される。画像出力部 55 はモニタ等の画像表示装置であってもよいし、あるいは磁気ディスク等の記憶装置であってもよい。

### 【0032】

以上述べた手順により画像を復元表示した際の、画像の表示形態について図 8

を用いて説明する。同図（a）は符号列の例を示したものであり、基本的な構成は図4に基づいているが、画像全体をタイルと設定されており、従って符号列中には唯一のタイルヘッダおよびビットストリームが含まれている。ビットストリームBS0には図に示すように、最も低い解像度に対応するサブバンドであるLLから順次解像度が高くなる順に符号が配置されている。

#### 【0033】

圧縮復号処理部はこのビットストリームを順次読み込み、各サブバンドに対応する符号を復号した時点で画像を表示する。同図（b）は各サブバンドと表示される画像の大きさの対応を示したものである。この例では2次元の離散ウェーブレット変換が2レベルであり、LLのみを復号・表示した場合は原画像に対して画素数が水平および垂直方向に1/4縮小された画像が復元される。更にビットストリームを読み込み、レベル2のサブバンド全てを復号して表示した場合は、画素数が各方向に1/2に縮小された画像が復元され、レベル1のサブバンド全てが復号されれば、原画像と同じ画素数の画像が復元される。

#### 【0034】

上述した実施の形態において、エン트로ピ復号部52において復号する下位ビットプレーンを制限（無視）することで受信或いは処理する符号化データ量を減少させ、結果的に圧縮率を制御することが可能である。この様にすることにより、必要なデータ量の符号化データのみから所望の画質の復号画像を得ることが可能である。また、符号化時の量子化ステップ $\Delta$ が1であり、復号時に全てのビットプレーンが復号された場合は、復元された画像が原画像と一致する可逆符号化・復号化を実現することもできる。

#### 【0035】

##### <暗号符号化処理部>

次に、図11を用いて本実施の形態に適応可能な暗号符号化処理部について説明する。

#### 【0036】

図11において、111は符号入力部、112は暗号化処理部、113は符号出力部である。図示において、符号入力部111は、図1における符号出力部1

5 の出力結果を入力するものと考えれば分かりやすい。

#### 【0037】

符号入力部 111 は符号列を入力し、それに含まれるヘッダを解析して後続の処理に必要なパラメータを抽出し、後続の処理ユニットに対して該当するパラメータを送出するものである。また符号列に含まれるビットストリームは暗号化処理部 112 に出力される。

#### 【0038】

暗号化処理部 112 には、前記ビットストリームが入力され、操作者の指定や予め設定された情報（例えばハードディスクに記憶しておく）に従って、前記ビットストリームが暗号化処理され、暗号化されたビットストリームが出力される。

#### 【0039】

ここで、暗号化処理部 112 で実行される暗号化処理について、図 12 を用いて説明する。図 12 は、本実施形態に適応可能な暗号化処理を示すフローチャートである。

#### 【0040】

まず、ステップ S121 において、入力されたビットストリームが誤り検出符号化されているか否かが判定される。これは、前段の符号入力部 111 において解析された符号化パラメータに含まれる第 1 の誤り検出符号化情報を用いて判定可能である。第 1 の誤り検出符号化情報が“1”の場合（誤り検出符号化されていると判定された場合）には処理をステップ S122 に進め、第 1 の誤り検出符号化情報が“0”の場合（誤り検出符号化されていないと判定された場合）には処理をステップ S124 に進める。

#### 【0041】

ステップ S122 では、前記第 1 の誤り検出符号化情報を“0”に変更する。即ち、あたかも「誤り検出符号化されていない」ような情報に変更する。これは、後述するステップ S124 における暗号化処理によって、圧縮復号処理部での誤り検出機能が、「誤りが生じている」と誤判定するのを防止するためである。第 1 の誤り検出符号化情報を“0”とすることにより、圧縮復号処理部で誤

り検出検出機能は動作しないが、「誤りが生じている」と誤判定することは防止できる。ステップS122の後、処理をステップS123に進める。

#### 【0042】

ステップS123では、前記第1の誤り検出符号化情報とは異なる第2の誤り検出符号化情報を“1”に設定する。第2の誤り検出符号化情報は、「暗号化される前のビットストリームが誤り検出符号化されているか否かを示す」情報である。第2の誤り検出符号化情報が“1”の場合には、暗号化される前のビットストリームが誤り検出符号化されていたことを示し、一方で、第2の誤り検出符号化情報が“0”の場合には、暗号化される前のビットストリームが誤り検出符号化されていなかったことを示す。第2の誤り検出符号化情報は、前述したステップS122において誤り検出符号化情報を変更したことを補うために、後述する暗号復号処理部において用いられる。つまり、元々存在していた誤り検出符号化情報を待避することと等価の処理を行う。

#### 【0043】

また、第2の誤り検出符号化情報はヘッダ部分や、或いは、ヘッダ部分に含まれるコメントとして記録したりすればよい。或いは、第2の誤り検出符号化情報をビットストリームの所定の位置に添付し、後段の暗号化処理においてビットストリームと共に暗号化し、暗号文の中に含まれるようにしても構わない。

#### 【0044】

さて、ステップS124では、入力されたビットストリームに暗号化処理が施される。暗号化処理としては、入力されたビットストリームに含まれるデータの全てを暗号化するようにしてもよいし、一部分だけを部分的に暗号化するようにしてもよい。部分的に暗号化することにより、暗号化されていない部分は誰でも閲覧可能であるが、暗号化された部分は許可されたユーザだけが閲覧可能となるようなアクセス制御が可能である。

#### 【0045】

本発明においては暗号化対象は特に限定されることなく、前述した所定のサブバンドやビットプレーンやタイルなどの種々のデータを暗号化対象とすることが可能であることは明らかである。また、本発明においては暗号化処理は特に限定

されることなく、DES、AES、RSAなどの種々の暗号化方式が適応可能であることは明らかである。

#### 【0046】

尚、本実施形態においてはステップS121、ステップS122、及びステップS123の後にステップS124を処理するようにしたが、ステップS124の後に、ステップS121、ステップS122、及びステップS123を処理するようにしてもよい。

#### 【0047】

以上説明したような処理により生成されたヘッダ情報や暗号化されたビットストリームは後段の符号出力部113に出力される。

#### 【0048】

符号出力部113には、前段の暗号化処理部112で生成されたヘッダ情報や暗号化されたビットストリームが入力され、暗号化された符号列として出力される。

#### 【0049】

以上説明したように本実施形態によれば、画像符号化データを入力し、暗号化を行った場合、例えば誤り訂正符号が付加されたとしても、誤り訂正符号無しにすることで、復号する側（例えばPC）が画像データに誤りがあると誤認識することを避けることができるようになる。

#### 【0050】

なお、上記暗号化する側で行った暗号化済みの符号化データを受信した、復号化する側の装置では、暗号化を解除しない限りは正常な画像データにまで復号できない。換言すれば、復号化する側の装置では、何らかの手段を用いて、暗号化解除鍵情報を取得する必要がある。簡単には、復号化する側が暗号化する側に対して解除鍵を要求することであろうが、例えば双方がインターネット等のネットワークに接続する形態を採っている場合には、画像データを特定する情報と解除鍵情報を管理する認証サーバを設置し、その画像を特定する情報を受信した場合にその解除鍵情報を要求元に送信する形態を採用すれば良いであろう。

#### 【0051】

以上、本実施形態における暗号符号化処理部における動作について説明した。上記本実施形態における暗号符号化処理部は、一般に、パーソナルコンピュータ等の情報処理装置で実現できることは容易に類推できよう。また、パーソナルコンピュータ等の情報処理装置で、上記機能を実現すれば良いわけであるから、実施形態での特徴は情報処理方法、更には、コンピュータプログラムや、コンピュータプログラムを格納するCDROM等のコンピュータ可読記憶媒体にまで及ぶものである。

#### 【0052】

##### <暗号復号処理部>

次に、図13を用いて本実施の形態に適応可能な暗号復号処理部について説明する。

#### 【0053】

図13において、131は符号入力部、132は暗号復号処理部、133は符号出力部である。図5に示す復号装置における符号入力部51は、符号出力部133から出力された符号データを入力すると考えると分かりやすい。

#### 【0054】

符号入力部131は符号列を入力し、それに含まれるヘッダを解析して後続の処理に必要なパラメータを抽出し、後続の処理ユニットに対して該当するパラメータを送出するものである。また符号列に含まれるビットストリームは暗号復号処理部132に出力される。

#### 【0055】

暗号復号処理部132には、前記ビットストリームが入力され、前記ビットストリームが暗号復号処理され、暗号復号処理されたビットストリームが出力される。

#### 【0056】

ここで、暗号復号処理部132で実行される暗号化処理について、図14を用いて説明する。図14は、本実施形態に適応可能な暗号復号処理を示すフローチャートである。

#### 【0057】

まず、ステップ S 1 4 1 において入力されたビットストリームが、暗号化前に誤り検出符号化されていたか否かが判定される。これは、前段の符号入力部 1 3 1 において解析されたヘッダなどに含まれる第 2 の誤り検出符号化情報を用いて判定可能である。第 2 の誤り検出符号化情報が“0”の場合（誤り検出符号化されていないと判定された場合）には、処理はステップ S 1 4 3 に進み、暗号解除鍵情報が存在するか否かを判定する。暗号化鍵情報がないと判断した場合には、本処理を終え、下位の処理にそのまま符号化データを出力する。また、暗号化鍵情報が存在すると判断した場合には、ステップ S 1 4 5 で暗号化を解除する処理（暗号復号化処理）を行った後、下位に出力する。

#### 【0058】

一方、ステップ S 1 4 1 において入力されたビットストリームが、暗号化前に誤り検出符号化されていたと判断した場合、処理はステップ S 1 4 2 に進み、暗号化鍵情報が存在するか否かを判断する。暗号化鍵情報が存在しない場合には本処理を終える。つまり、ステップ S 1 4 3 での N o と判断された場合と同様になる。

#### 【0059】

また、暗号化鍵情報が存在すると判断した場合、処理をステップ S 1 4 4 に進め、第 1 の誤り検出符号化情報を“0”から“1”に変更する。即ち、「誤り検出符号化されている」ような情報に変更する。これは、第 1 の誤り検出符号化情報を“1”とすることにより、圧縮復号処理部において、再び誤り検出機能を動作させるための処理である。

#### 【0060】

そして、ステップ S 1 4 5 では、入力されたビットストリームに暗号解除鍵情報に基づいて暗号復号処理が施される。暗号復号処理は前述したステップ S 1 2 4 における暗号化処理に対応したものでなければならない。

#### 【0061】

以上説明したような処理により生成されたヘッダ情報や暗号化されたビットストリームは後段の符号出力部 1 3 3 に出力される。

#### 【0062】

尚、本実施形態においては、第1の誤り検出符号化情報を変更した後に、暗号復号処理を実行するようにしたが、本発明はこれに限定されることなく、図15に示すように暗号復号処理を実行した後に、第1の誤り検出符号化情報を変更するようにしても良い。

#### 【0063】

特に、前述した暗号符号化処理部において、第2の誤り検出符号化情報を暗号文の中に含めるようにした場合には、図15に示すようなフローに従って暗号復号処理を実行する必要がある。これは、第2の誤り検出符号化情報が暗号文の中に含まれている為に、暗号化されている状態では、正しく第2の誤り検出符号化情報を調べるのが困難だからである。

#### 【0064】

そして、符号出力部133には、前段の暗号復号処理部132で生成されたヘッダ情報や暗号復号されたビットストリームが入力され、暗号復号された符号列として出力される。尚、復号出力部は、更に、前述した圧縮復号出力部に接続され、引き続き圧縮復号処理が実行されるようにしてもよい。

#### 【0065】

以上説明したように本実施形態によれば、暗号符号化処理を行うことによって、暗号符号化処理された符号列が、誤りが生じていると誤判定されないようにすることが可能となる。

#### 【0066】

より分かりやすく説明するのであれば、暗号化する装置側で、誤り検出符号を付加したとしても、暗号化処理を行う場合には、見かけ上誤り検出符号データが存在しないことになる（実際には誤り検出符号データは存在するが無視されるだけ）。従って、正しく伝送されている限りは、復号化する装置側では、データに誤りがあると誤判定し、再送の要求を行うことはなくなる。

#### 【0067】

また、復号化する装置側が暗号化鍵を解除する解除鍵情報を取得している場合には、暗号化が解除（復号）され、誤り検出の符号を利用できるようになるので、万が一、データ伝送中にノイズが入ったとしても、再送を要求し、正常な画像

を再現できるようになる。以上、本実施形態における暗号復号処理部における動作について説明した。

#### 【0068】

上記本実施形態における暗号復号処理部は、一般に、パーソナルコンピュータ等の情報処理装置で実現できることは容易に類推できよう。また、パーソナルコンピュータ等の情報処理装置で、上記機能を実現すれば良いわけであるから、実施形態での特徴は情報処理方法、更には、コンピュータプログラムや、コンピュータプログラムを格納するCDROM等のコンピュータ可読記憶媒体にまで及ぶものである。

#### 【0069】

##### [第2の実施形態]

上記実施形態（第1の実施形態）では、暗号化前に誤り検出符号化されていたか否かを示す第2の誤り検出符号化情報を必要としたが、本発明はこれに限定されることなく、第2の誤り検出符号化情報を必要としないようにすることも可能である。そこで本第2の実施形態では、第2の誤り検出符号化情報を必要としない方法について説明する。

#### 【0070】

##### <暗号符号化処理部>

まず、図16を用いて本実施の形態における暗号符号化処理部について説明する。

#### 【0071】

図16において、161は符号入力部、162はエントロピ復号部、163は暗号化処理部、164はエントロピ符号化部、165は符号出力部である。

#### 【0072】

符号入力部161、エントロピ復号部162、エントロピ符号化部164、及び符号出力部165で実行される各々の処理は、第1の実施形態における符号入力部51、エントロピ復号部52、エントロピ符号化部14、及び符号出力部15で実行される処理と夫々等しいため、詳細な説明は省略する。そこで、本第2の実施形態では処理が異なる暗号化処理部163における暗号化処理についての

詳細を説明する。

#### 【0073】

図17は本実施形態に適応可能な暗号化処理を示すフローチャートである。

#### 【0074】

まず、ステップS171においてエントロピ復号部162を用いてビットプレーン毎に前述したエントロピ復号処理が実行される。続いてステップS172においてエントロピ復号されたデータに対して暗号化処理が実行される。

#### 【0075】

次に、ステップS173で、入力されたビットストリームが誤り検出符号化されているか否かが判定される。これは、前段の符号入力部161において解析された符号化パラメータに含まれる第1の誤り検出符号化情報を用いて判定可能である。第1の誤り検出符号化情報が“1”の場合（誤り検出符号化されていると判定された場合）には処理をステップS174に進み、第1の誤り検出符号化情報が“0”の場合（誤り検出符号化されていないと判定された場合）には処理をステップS175に進める。

#### 【0076】

ステップS174では、前段のステップS172において暗号化処理が施されたデータの後ろにセグメンテーションシンボルを添付する。これにより、暗号化されたデータに対して誤り検出機能を持たせることが可能である。

#### 【0077】

ステップS175では、暗号化されたデータに対してエントロピ符号化部164を用いてビットプレーン毎にエントロピ符号化処理を施す。前段のステップS174においてセグメンテーションシンボルが添付されている場合には、セグメンテーションシンボルも含めてエントロピ符号化処理を施すようにする。

#### 【0078】

以上説明したような処理により生成されたヘッダ情報や暗号化されたビットストリームは後段の符号出力部165に出力される。

#### 【0079】

<暗号復号処理部>

次に、実施形態における画像データを復号化（再生する）側の処理について説明する。

#### 【0080】

図18は本第2の実施形態に適応可能な暗号復号処理部のブロック構成図である。同図において、181は符号入力部、182はエントロピ復号部、183は暗号復号部、184はエントロピ符号化部、185は符号出力部である。図5における符号入力部51は、符号化部185から出力されるデータを入力すると考えると分かりやすい。

#### 【0081】

第1の実施形態（図13）と処理が異なるのは、暗号復号処理部163と、その前後にエントロピー復号部163、エントロピー符号化部164を設けた点である。エントロピー復号部163、同符号化部164については、暗号化装置での処理と同じであるので、ここでは、暗号復号部183における暗号復号処理についての詳細を図19を用いて説明する。

#### 【0082】

まず、ステップS191において、暗号化解除鍵情報が存在するか否かを判断する。否の場合には、本処理を終える。

#### 【0083】

また、暗号化解除鍵情報が存在する場合、処理はステップS192に進み、エントロピ復号部182を用いてビットプレーン毎に前述したエントロピ復号処理が実行される。続いてステップS193においてエントロピ復号されたデータに対して暗号復号処理が実行される。そして、ステップS193で実行される暗号復号処理は、前述したステップS172に対応する処理でなければならない。そしてステップS194においてエントロピ符号化部184を用いてビットプレーン毎に前述したエントロピ符号化処理が実行される。

#### 【0084】

以上説明したような処理により生成されたヘッダ情報や暗号復号されたビットストリームは後段の符号出力部185に出力され、図5で示される処理に渡されることになる。

## 【0085】

以上説明したように暗号符号化処理を行うことによって、暗号化されたデータに対しても誤り検出符号化機能を有するようにすることが可能となる。

## 【0086】

以上、本実施形態における暗号符号化処理部、及び暗号復号処理部における動作について説明した。上記本実施形態における暗号符号化処理部、暗号復号処理部は、一般に、パーソナルコンピュータ等の情報処理装置で実現できることは容易に類推できよう。また、パーソナルコンピュータ等の情報処理装置で、上記機能を実現すれば良いわけであるから、実施形態での特徴は情報処理方法、更には、コンピュータプログラムや、コンピュータプログラムを格納するCDROM等のコンピュータ可読記憶媒体にまで及ぶものである。

## 【0087】

## [第3の実施形態]

上記第2の実施形態においては、JPEG2000などを想定して誤り検出符号化処理が、エントロピー符号化（図1におけるエントロピー符号化部14）内で実行される例を説明した。しかしながら本発明はこれに限定されることない。すなわち、暗号化した際の、誤り検出符号の付加を単独で実行するようにしても良い。以下、この例を第3の実施形態として説明する。

## 【0088】

## &lt;暗号符号化処理部&gt;

まず、図20を用いて本実施の形態における暗号符号化処理部（暗号符号化装置）について説明する。

## 【0089】

図20において、201は符号入力部、202は暗号符号化部、203は誤り検出符号化部、204は符号出力部である。符号化部201は、図1における符号化部15の出力結果を入力するものとする。と分かりやすいが、符号入力部201が入力する符号化ストリームはこれに限らず、他の圧縮符号化処理で生成されたものでも良い。

## 【0090】

図 21 は本実施形態に適応可能な暗号化処理、及び誤り訂正符号化処理を示すフローチャートである。

#### 【0091】

まず、ステップ S 211 で、暗号化処理部 202 を用いて、入力されたビットストリームに対して暗号化処理が実行される。注意したいのは、入力したビットストリームは、画像データそのものの符号化データに、誤り検出符号が付加されている場合と、それが付加されていない場合がある点である。また、ここで言う暗号化処理は、入力した符号化データが「画像データの符号化データ+誤り検出符号データ」である場合には、その誤り検出を含めて暗号化する。誤り検出符号が存在しない場合には、当然暗号化対象は「画像データの符号化データ」のみとなる。従って、入力した符号化データが「画像データの符号化データ+誤り検出符号データ」である場合には、暗号化後にはその区別がない 1 つのストリームが生成されることになる。

#### 【0092】

次いで、ステップ S 212 に進み、暗号化処理を行った符号化データに誤り検出符号データが存在したか否かを判断する。この判断は、第 1、第 2 の実施形態で述べた、第 1 の誤り検出符号化情報を参照する等で対処できるであろうし、場合によっては現実に誤り検出符号データを検出できたか否かで判断してもよい。

#### 【0093】

いずれにせよ、「誤り検出符号データ」というのは、画像符号化データの信頼性を高めたいという現れである。従って、ステップ S 212 での判断で YES になった場合には、暗号化したデータの伝送の信頼性を高くするため、ステップ S 213 で誤り検出符号化をおこなう。また、ステップ S 212 で NO になった場合には、もともと誤り検出符号が行われていないわけであるから、ステップ S 213 の処理はおこなわない。

#### 【0094】

以上説明したように暗号符号化処理を行うことによって、暗号化されたデータに対しても誤り訂正符号化機能を有するようにすることが可能となる。

#### 【0095】

以上、本実施形態における暗号符号化処理部、及び暗号復号処理部における動作について説明した。上記本実施形態における暗号符号化処理部、暗号復号処理部は、一般に、パーソナルコンピュータ等の情報処理装置で実現できることは容易に類推できよう。また、パーソナルコンピュータ等の情報処理装置で、上記機能を実現すれば良いわけであるから、実施形態での特徴は情報処理方法、更には、コンピュータプログラムや、コンピュータプログラムを格納するCDROM等のコンピュータ可読記憶媒体にまで及ぶものである。

#### 【0096】

以上本発明にかかる実施形態を説明したが、上記実施形態に係る実施態様を列挙すると、次の通りである。

#### 【0097】

[実施態様1] 符号化画像データを暗号化する情報処理方法であって、  
符号化画像データを入力する工程と、  
入力した符号化画像データを暗号化する工程と、  
符号化データのヘッダ部中の誤り検出符号有無を示す有無情報を、誤り検出符号無しに変更し、暗号化した符号化画像データを出力する工程と  
を備えることを特徴とする情報処理方法。

#### 【0098】

[実施態様2] 更に、暗号化を解除する暗号化解除鍵情報を出力する工程を備えることを特徴とする実施態様1に記載の情報処理方法。

#### 【0099】

[実施態様3] 更に、入力した符号化画像データ中の前記有無情報を、前記ヘッダ部内の他の位置に待避する工程を備えることを特徴とする実施態様1に記載の情報処理方法。

#### 【0100】

[実施態様4] 前記待避する工程では、前記ヘッダ部にコメントとして待避することを特徴とする実施態様2に記載の情報処理方法。

#### 【0101】

[実施態様5] 実施態様3に記載の情報処理方法で暗号化された画像デー

タを復号する情報処理方法であって、  
符号化画像データを入力する工程と、  
前記待避した前記有無情報が、誤り検出有りを示すか否かを判定する第1の判定工程と、  
暗号化を解除する鍵情報があるか否かを判定する第2の判定工程と、  
前記第1、第2の判定工程によって、誤り検出符号有り、及び、暗号化解除鍵情報有りと判定した場合、前記ヘッダ部内の有無情報を誤り検出有りに変更すると共に、暗号化を解除し、符号化画像データの復号処理に渡す工程と  
を備えることを特徴とする情報処理方法。

#### 【0102】

【実施態様6】 前記第1、第2の判定工程によって、誤り検出符号無し、及び、暗号化解除鍵情報有りと判定した場合には、前記ヘッダ部内の有無情報を変更せず、暗号化を解除することを特徴とする実施態様5に記載の情報処理方法。

#### 【0103】

【実施態様7】 前記第1、第2の判定工程によって、暗号化解除鍵情報無しと判定した場合には、入力した符号化画像データをそのまま符号化画像データの復号処理に渡すことを特徴とする実施態様5に記載の情報処理方法。

#### 【0104】

【実施態様8】 符号化画像データを暗号化する情報処理装置であって、  
符号化画像データを入力する手段と、  
入力した符号化画像データを暗号化する手段と、  
符号化データのヘッダ部中の誤り検出符号有無を示す有無情報を、誤り検出符号無しに変更し、暗号化した符号化画像データを出力する手段と  
を備えることを特徴とする情報処理装置。

#### 【0105】

【実施態様9】 更に、入力した符号化画像データ中の前記有無情報を、前記ヘッダ部内の他の位置に待避する手段を備えることを特徴とする実施態様8に記載の情報処理装置。

## 【0106】

【実施態様10】 実施態様9に記載の情報処理装置で暗号化された画像データを復号する情報処理装置であって、  
符号化画像データを入力する手段と、  
前記待避した前記有無情報が、誤り検出有りを示すか否かを判定する第1の判定手段と、  
暗号化を解除する鍵情報があるか否かを判定する第2の判定手段と、  
前記第1、第2の判定工程によって、誤り検出符号有り、及び、暗号化解除鍵情報有りと判定した場合、前記ヘッダ部内の有無情報を誤り検出有りに変更すると共に、暗号化を解除し、符号化画像データの復号処理に渡す手段と  
を備えることを特徴とする情報処理装置。

## 【0107】

【実施態様11】 コンピュータが読み込み実行することで、符号化画像データを暗号化する情報処理装置として機能するコンピュータプログラムであって、  
符号化画像データを入力する手段と、  
入力した符号化画像データを暗号化する手段と、  
符号化データのヘッダ部中の誤り検出符号有無を示す有無情報を、誤り検出符号無しに変更し、暗号化した符号化画像データを出力する手段と  
して機能することを特徴とするコンピュータプログラム。

## 【0108】

【実施態様12】 更に、入力した符号化画像データ中の前記有無情報を、前記ヘッダ部内の他の位置に待避する手段として機能することを特徴とする実施態様11に記載のコンピュータプログラム。

## 【0109】

【実施態様13】 実施態様11又は12に記載のコンピュータプログラムを格納することを特徴とするコンピュータ可読記憶媒体。

## 【0110】

【実施態様14】 コンピュータが読み込み実行することで、実施態様9に

記載の情報処理装置で暗号化された画像データを復号する情報処理装置として機能するコンピュータプログラムであって、

符号化画像データを入力する手段と、

前記待避した前記有無情報が、誤り検出有りを示すか否かを判定する第1の判定手段と、

暗号化を解除する鍵情報があるか否かを判定する第2の判定手段と、

前記第1、第2の判定工程によって、誤り検出符号有り、及び、暗号化解除鍵情報有りと判定した場合、前記ヘッダ部内の有無情報を誤り検出有りに変更すると共に、暗号化を解除し、符号化画像データの復号処理に渡す手段と

して機能することを特徴とするコンピュータプログラム。

#### 【0111】

【実施態様15】 実施態様14に記載のコンピュータプログラムを格納することを特徴とするコンピュータ可読記憶媒体。

#### 【0112】

【実施態様16】 符号化画像データを暗号化する情報処理方法であって、符号化画像データを入力する工程と、

入力した圧縮符号化画像データを復号し、暗号化する工程と、

入力した圧縮符号化画像データのヘッダ部中の誤り検出符号の有無を示す有無情報を判定する工程と、

該判定工程で誤り検出符号無しと判定した場合には暗号化した画像データを再符号化し、誤り検出符号有りと判定した場合、前記暗号化工程で暗号化した画像データに誤り検出符号有りを示すセグメンテーションシンボルを付加して再符号化する再符号化制御工程と

を備えることを特徴とする情報処理方法。

#### 【0113】

【実施態様17】 前記復号工程はエントロピー復号、前記再符号化制御工程ではエントロピー符号を行うことを特徴とする実施態様16に記載の情報処理方法。

#### 【0114】

【実施態様 18】 実施態様 16 又は実施態様 17 に記載の情報処理方法で暗号化、符号化された画像データを復号するための情報処理方法であって、

暗号化され、符号化画像データを入力する工程と、

暗号化状態に復元するため、前記入力工程で入力した符号化画像データを復号する工程と、

暗号化を解除する鍵情報に基づいて暗号化を解除し、再符号化を行う符号化工程と、

再符号化した符号化データを、下位に位置する圧縮符号化画像データの復号処理に出力する工程とを備えることを特徴とする情報処理方法。

#### 【0115】

【実施態様 19】 符号化画像データを暗号化する情報処理装置であって、符号化画像データを入力する手段と、

入力した圧縮符号化画像データを復号し、暗号化する手段と、

入力した圧縮符号化画像データのヘッダ部中の誤り検出符号の有無を示す有無情報を判定する手段と、

該判定手段で誤り検出符号無しと判定した場合には暗号化した画像データを再符号化し、誤り検出符号有りと判定した場合、前記暗号化手段で暗号化した画像データに誤り検出符号有りを示すセグメンテーションシンボルを付加して再符号化する再符号化制御手段と

を備えることを特徴とする情報処理装置。

#### 【0116】

【実施態様 20】 前記復号手段はエントロピー復号、前記再符号化制御手段ではエントロピー符号を行うことを特徴とする実施態様 19 に記載の情報処理装置。

#### 【0117】

【実施態様 21】 実施態様 19 又は実施態様 20 に記載の情報処理装置で暗号化、符号化された画像データを復号するための情報処理装置であって、

暗号化され、符号化画像データを入力する手段と、

暗号化状態に復元するため、前記入力工程で入力した符号化画像データを復号

する手段と、

暗号化を解除する鍵情報に基づいて暗号化を解除し、再符号化を行う符号化手段と、

再符号化した符号化データを、下位に位置する圧縮符号化画像データの復号処理に出力する手段と

を備えることを特徴とする情報処理装置。

#### 【0118】

【実施態様 22】 コンピュータが読み込み実行することで、符号化画像データを暗号化する情報処理装置として機能するコンピュータプログラムであって、

符号化画像データを入力する手段と、

入力した圧縮符号化画像データを復号し、暗号化する手段と、

入力した圧縮符号化画像データのヘッダ部中の誤り検出符号の有無を示す有無情報を判定する手段と、

該判定手段で誤り検出符号無しと判定した場合には暗号化した画像データを再符号化し、誤り検出符号有りとして判定した場合、前記暗号化手段で暗号化した画像データに誤り検出符号有りを示すセグメンテーションシンボルを付加して再符号化する再符号化制御手段と

して機能することを特徴とするコンピュータプログラム。

#### 【0119】

【実施態様 23】 前記復号手段はエントロピー復号、前記再符号化制御手段ではエントロピー符号を行うことを特徴とする実施態様 22 に記載のコンピュータプログラム。

#### 【0120】

【実施態様 24】 実施態様 22 又は実施態様 23 に記載のコンピュータプログラムを格納することを特徴とするコンピュータ可読記憶媒体。

#### 【0121】

【実施態様 25】 コンピュータが読み込み実行することで、実施態様 19 又は実施態様 20 に記載の情報処理装置で暗号化、符号化された画像データを復

号するための情報処理装置として機能するコンピュータプログラムであって、  
暗号化され、符号化画像データを入力する手段と、  
暗号化状態に復元するため、前記入力工程で入力した符号化画像データを復号  
する手段と、  
暗号化を解除する鍵情報に基づいて暗号化を解除し、再符号化を行う符号化手  
段と、  
再符号化した符号化データを、下位に位置する圧縮符号化画像データの復号処  
理に出力する手段と  
して機能することを特徴とするコンピュータプログラム。

**【0122】**

【実施態様26】 実施態様25に記載のコンピュータプログラムを格納す  
ることを特徴とするコンピュータ可読記憶媒体。

**【0123】****【発明の効果】**

以上説明したように本発明によれば、誤り検出符号が付加された圧縮符号化画  
像データを暗号化したとしても、それを受信し再生する側の装置において無意味  
な再送要求等を行わず、正常な処理を行えるようになる。

**【図面の簡単な説明】****【図1】**

実施形態における圧縮符号化処理部の構成を示す図である。

**【図2】**

実施形態における離散ウェーブレット変換部を説明する図である。

**【図3】**

実施形態におけるエントロピ符号化の説明をする図である。

**【図4】**

実施形態における符号列の説明をする図である。

**【図5】**

実施形態における圧縮復号処理部の構成を示す図である。

**【図6】**

実施形態におけるエントロピ復号の説明をする図である。

【図 7】

実施形態における逆離散ウェーブレット変換部を説明する図である。

【図 8】

実施形態における階層的な圧縮復号を説明する図である。

【図 9】

実施形態におけるシステム全体の構成図である。

【図 10】

実施形態における誤り検出符号付きのデータの構造を示す図である。

【図 11】

第 1 の実施形態における暗号符号化処理部の構成を示す図である。

【図 12】

第 1 の実施形態における暗号化処理手順を示すフローチャートである。

【図 13】

第 1 の実施形態における暗号復号処理部の構成を示す図である。

【図 14】

第 1 の実施形態における暗号復号処理手順を示すフローチャートである。

【図 15】

第 1 の実施形態における暗号復号処理の他のフローチャートである。

【図 16】

第 2 の実施形態における暗号符号化処理部の構成を示す図である。

【図 17】

第 2 の実施形態における暗号化処理手順を示すフローチャートである。

【図 18】

第 2 の実施形態における暗号復号処理部の構成を示す図である。

【図 19】

第 2 の実施形態における暗号復号処理手順を示すフローチャートである。

【図 20】

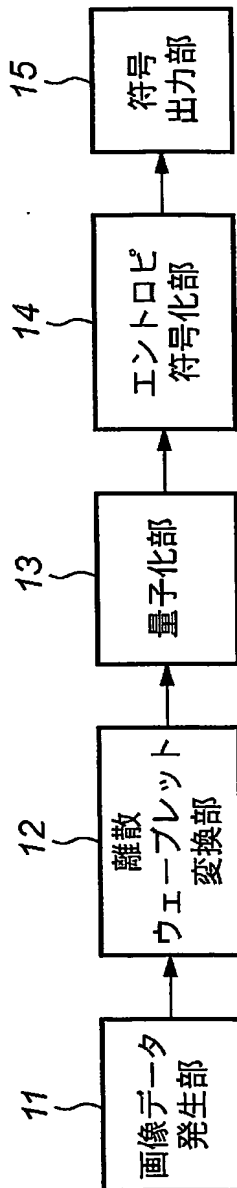
第 3 の実施形態における暗号符号化処理の構成を説明する図である。

【図 2 1】

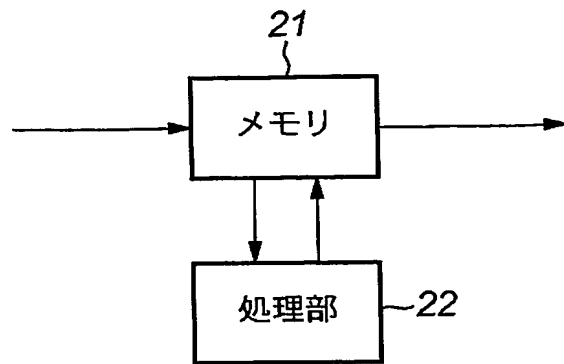
第 3 の実施形態における暗号符号化処理、及び誤り訂正符号化処理手順を示すフローチャートである。

【書類名】 図面

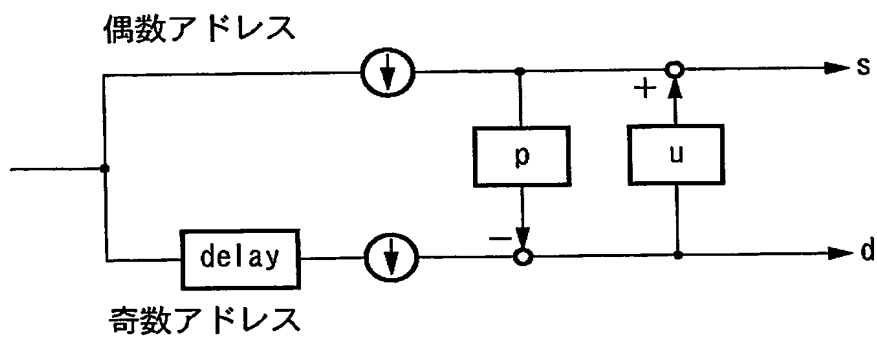
【図 1】



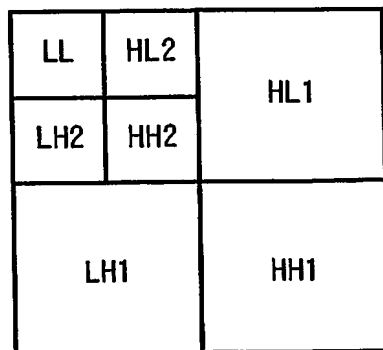
【図 2】



(a)

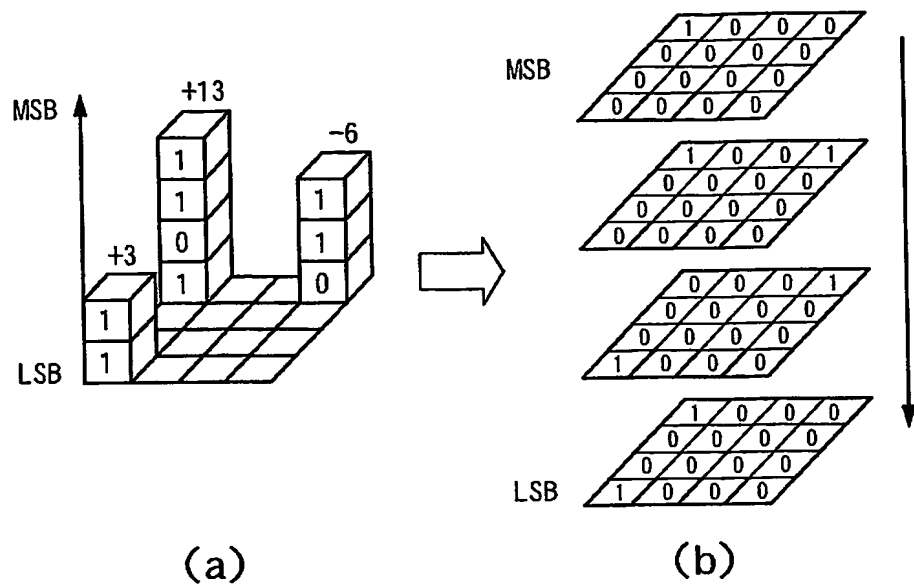


(b)

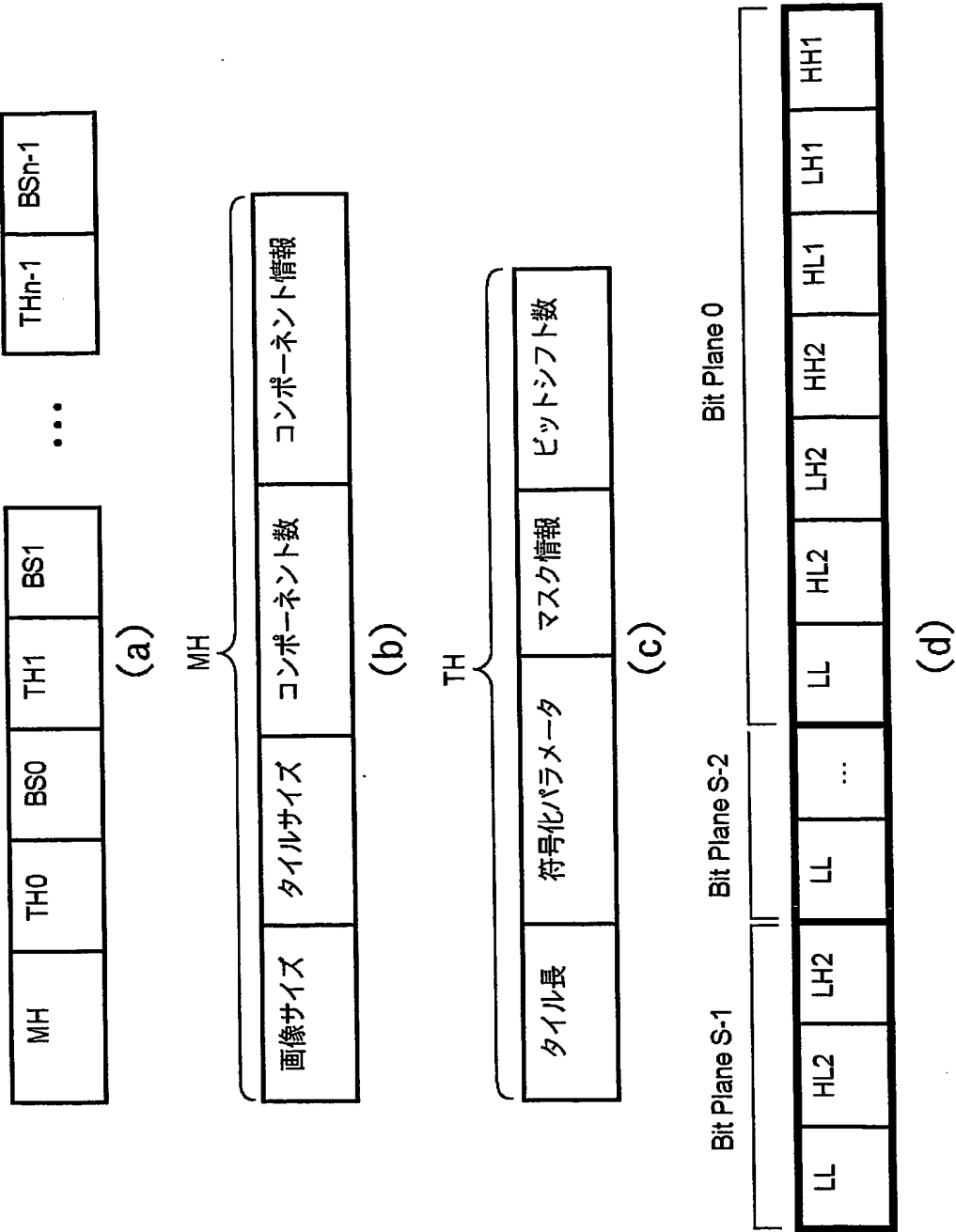


(c)

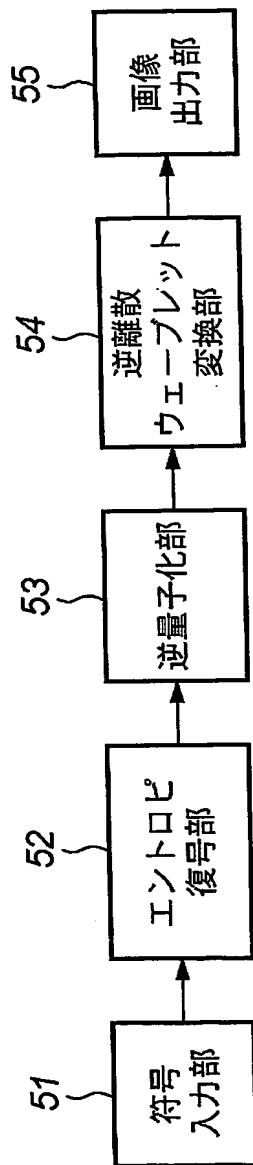
【図 3】



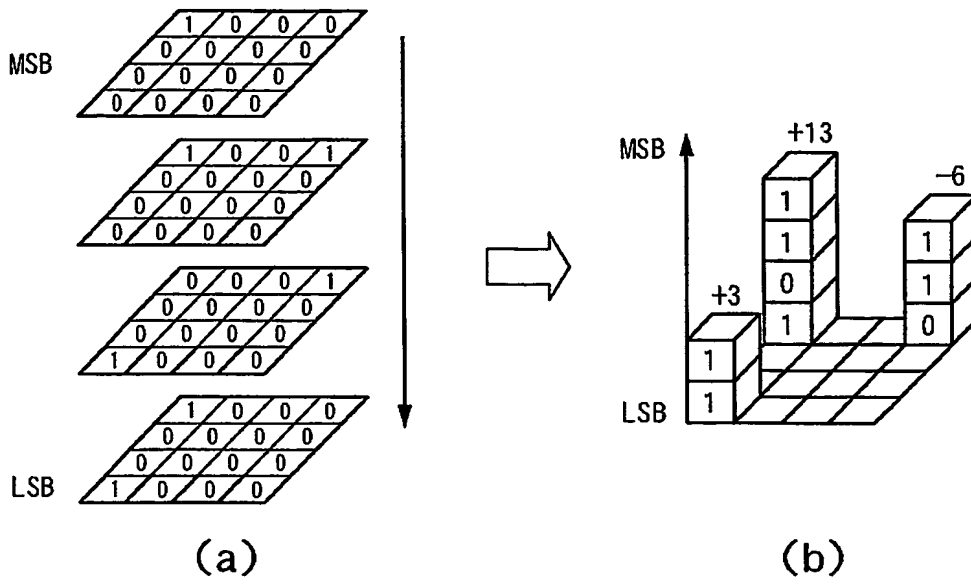
【図4】



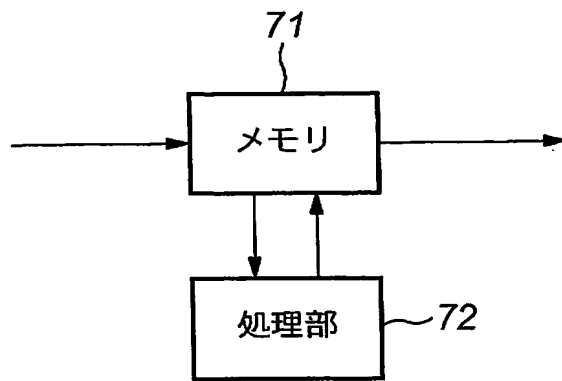
【図 5】



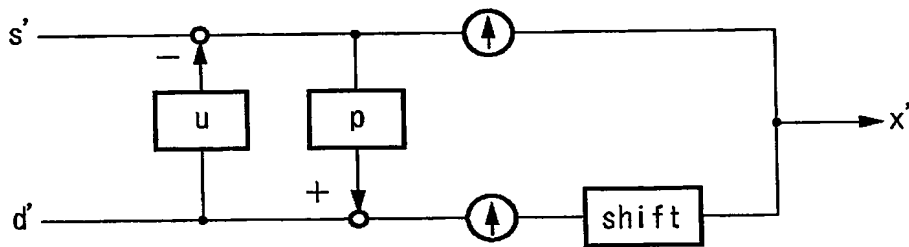
【図 6】



【図 7】

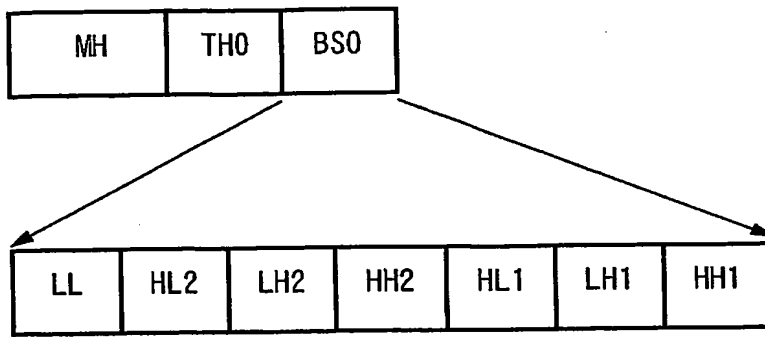


(a)



(b)

【図 8】



(a)

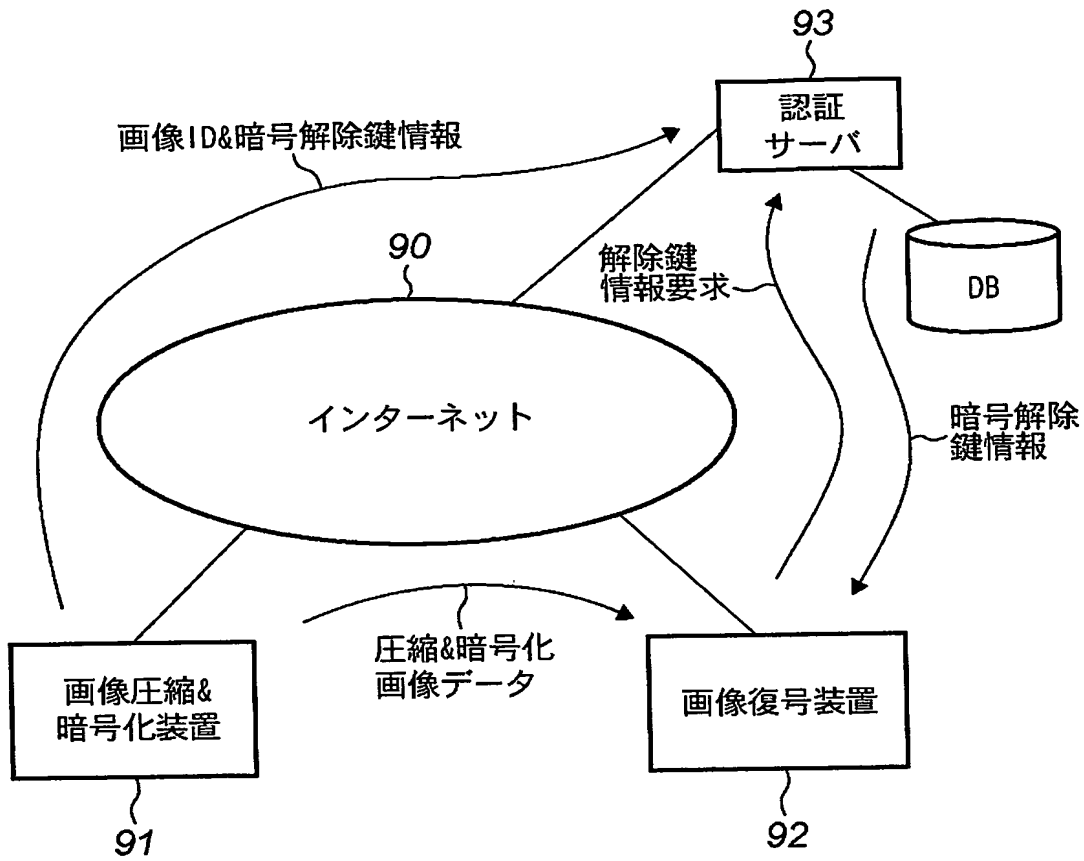
ABC = LL

ABC = LL+HL2+LH2+HH2

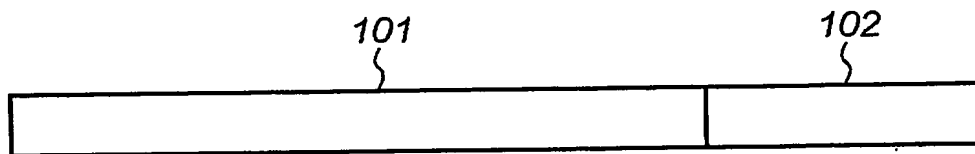
ABC = LL+HL2+LH2+HH2+HL1+LH1+HH1

(b)

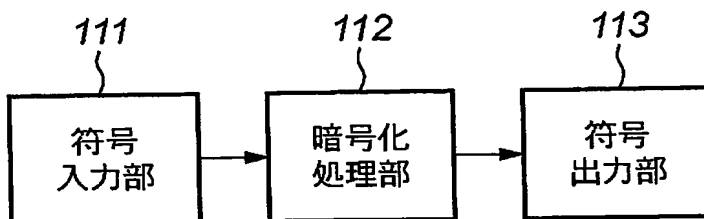
【図9】



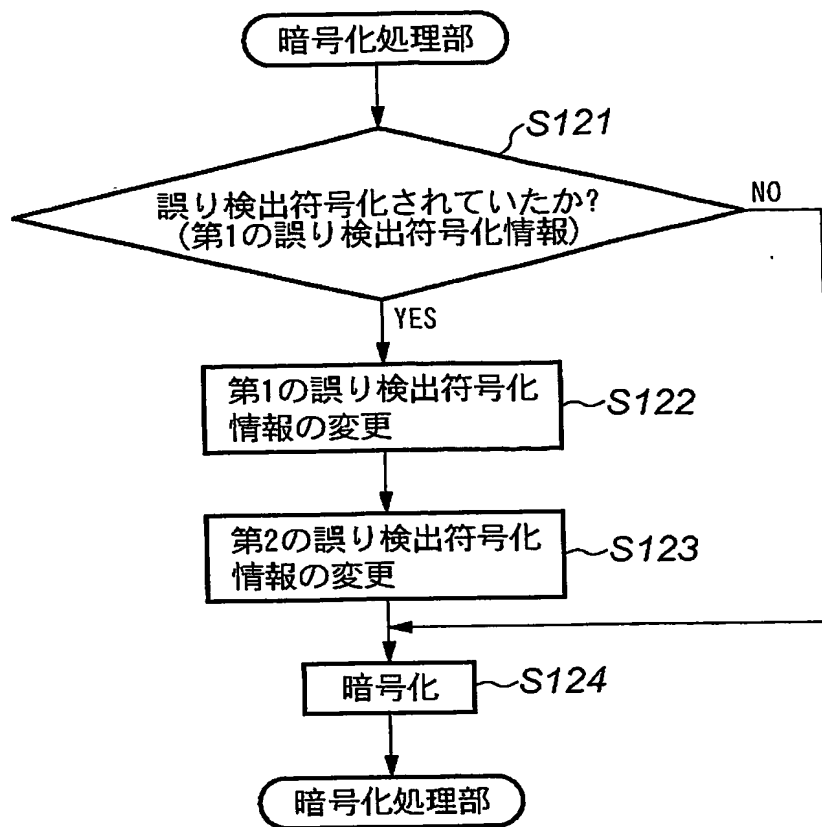
【図10】



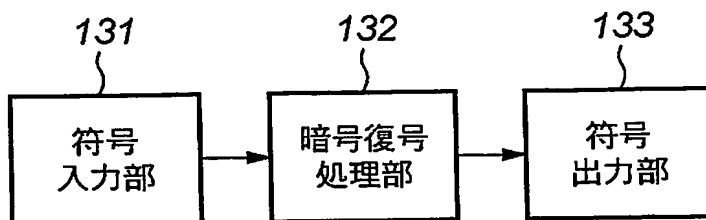
【図11】



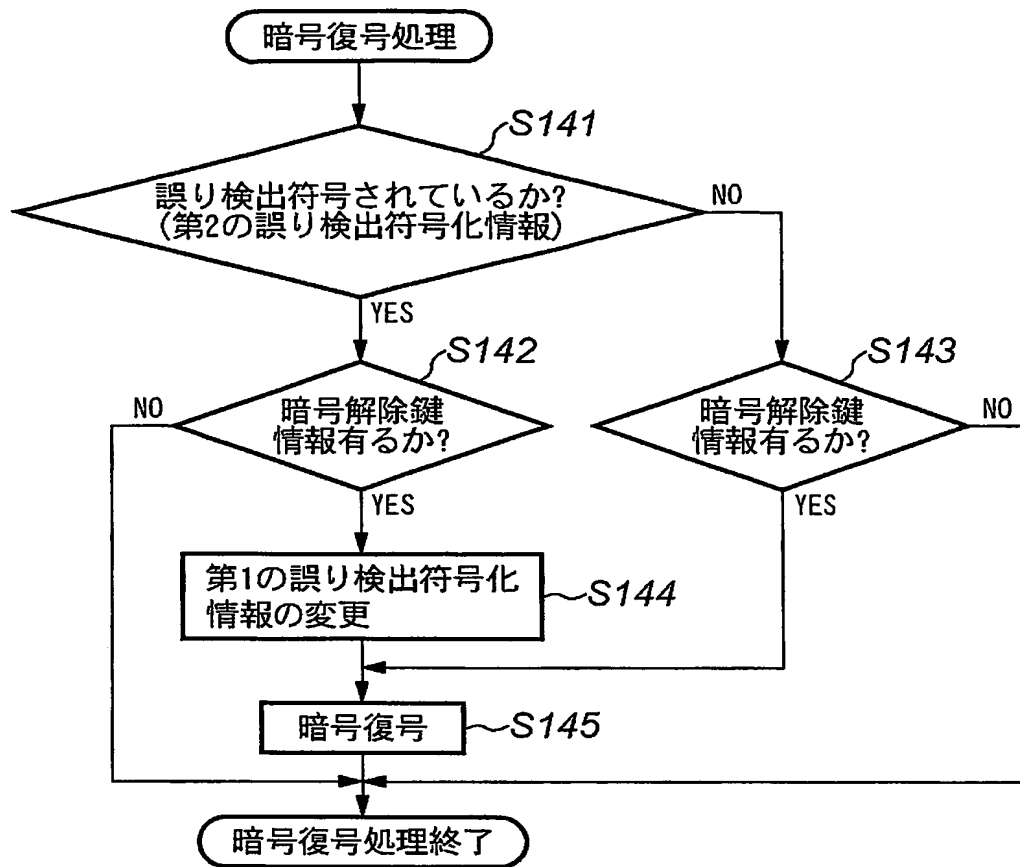
【図 1 2】



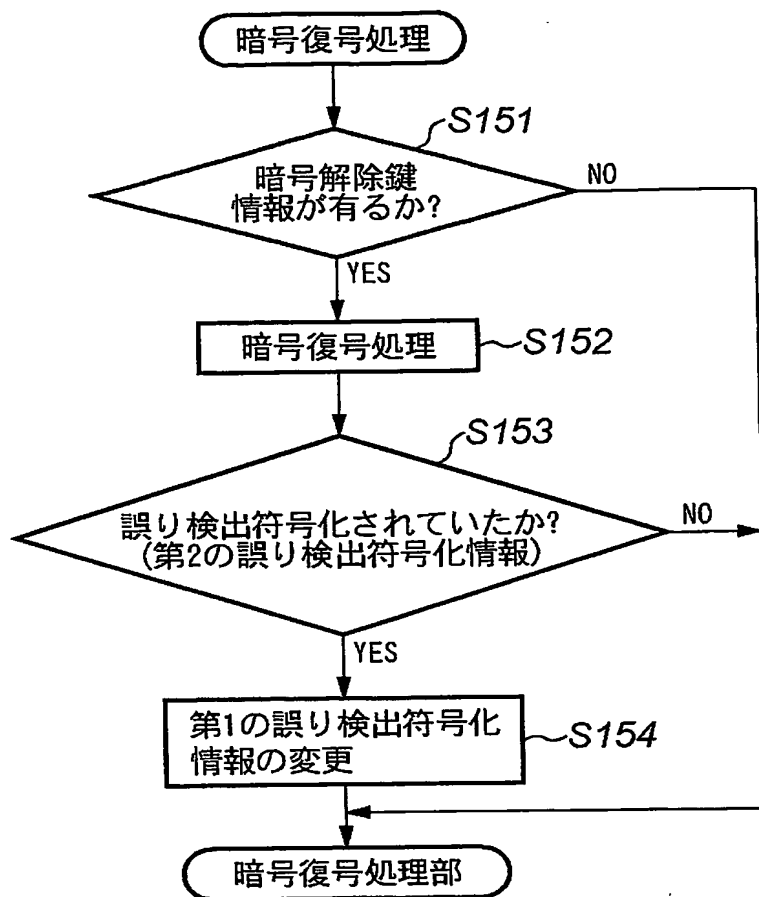
【図 1 3】



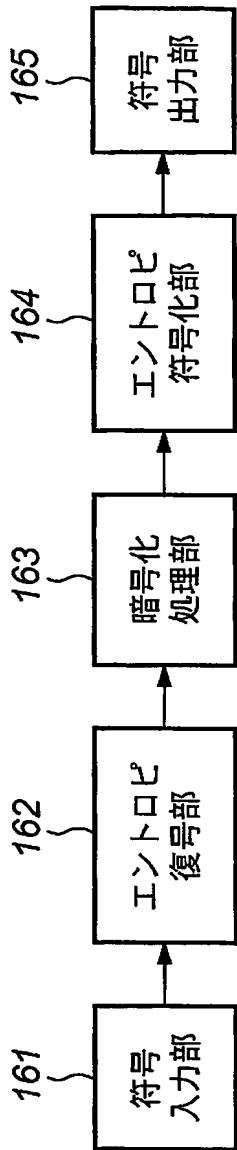
【図 14】



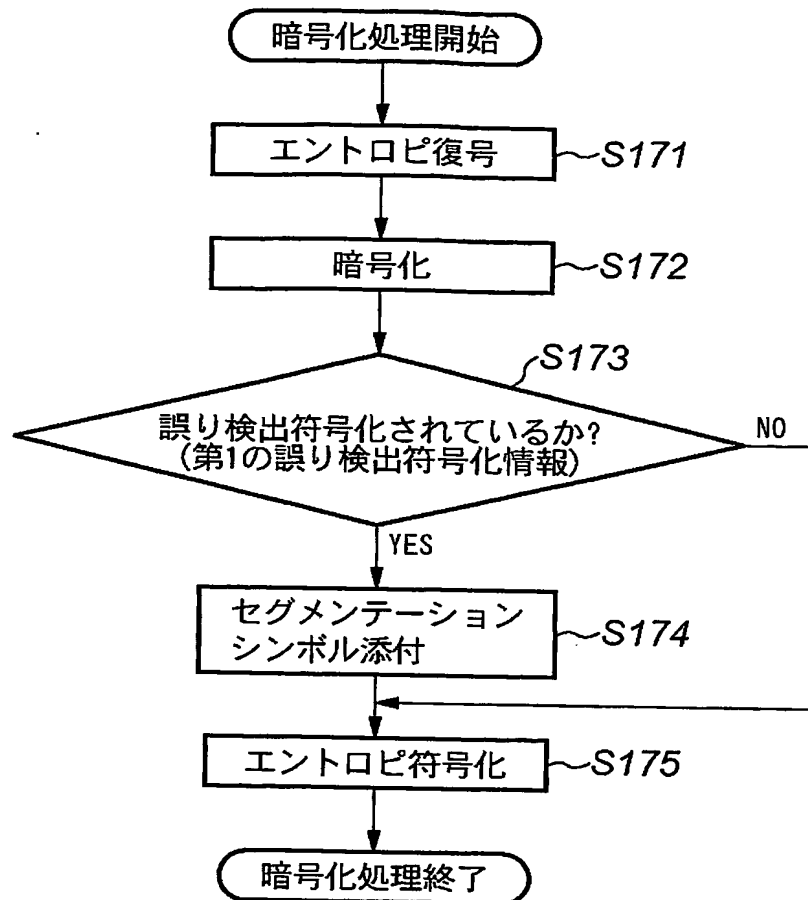
【図 15】



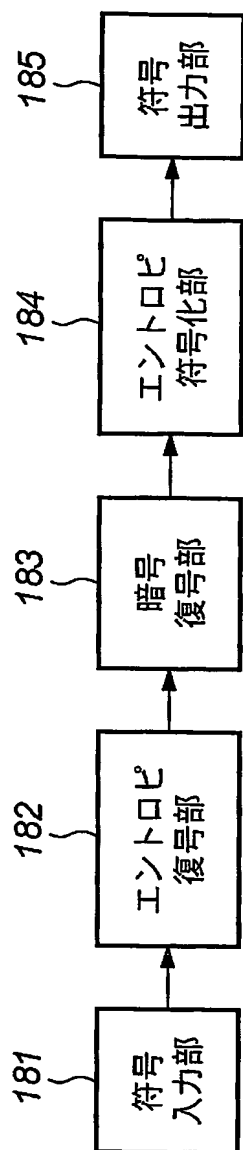
【図 16】



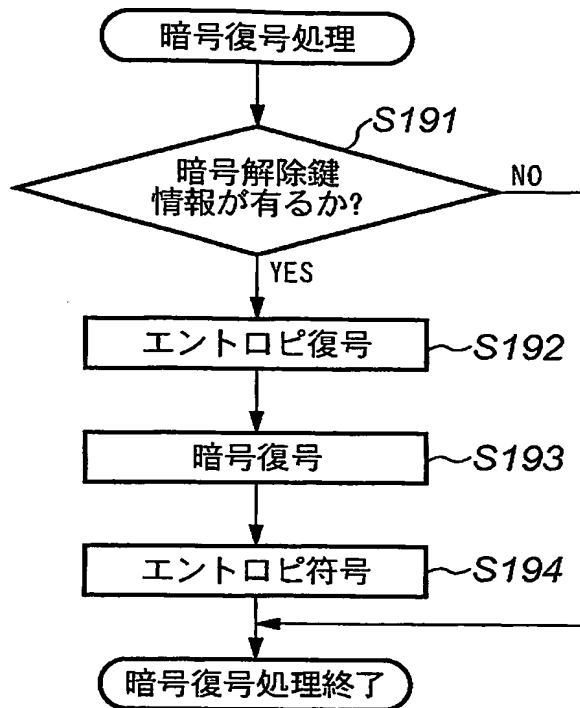
【図 17】



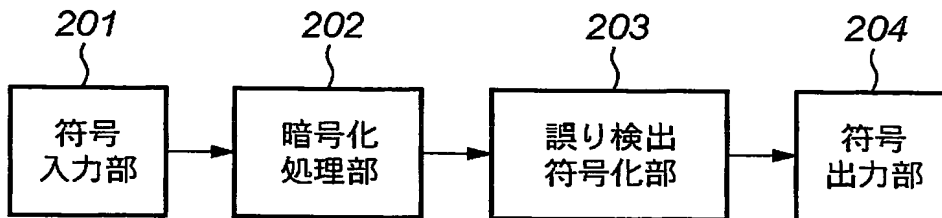
【図 18】



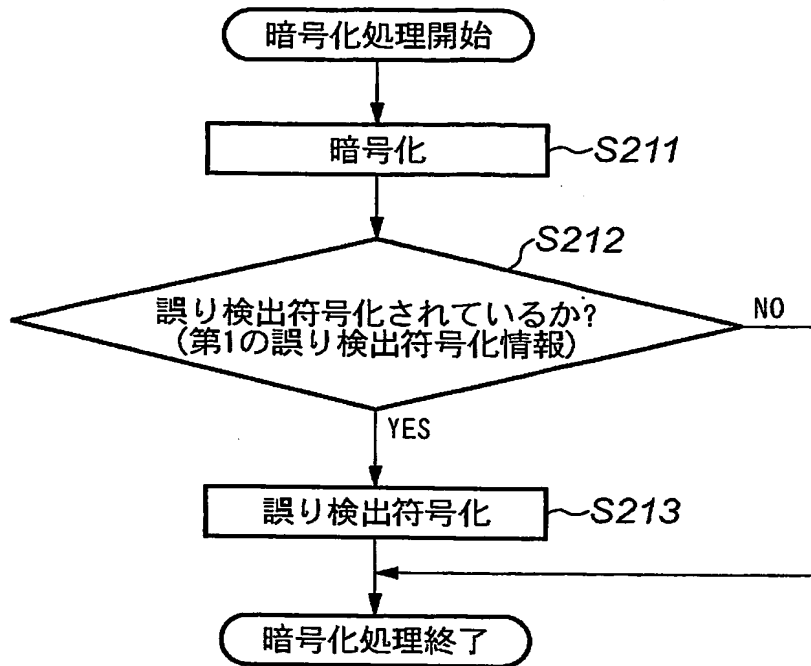
【図 19】



【図 20】



【図 21】



【書類名】 要約書

【課題】 誤り検出符号が付加された圧縮符号化画像データを暗号化したとしても、それを受信し再生する側の装置において無意味な再送要求等を行わず、正常な処理を行えるようになる。

【解決手段】 圧縮符号化された画像データを入力し、そのヘッダ部にある第1の誤り検出符号情報を調べることで、誤り検出符号が付加されているか否かを判定する（S 1 2 1）。誤り検出符号が付加されていると判断した場合には、その第1の誤り検出符号情報を誤り検出符号無しに変更し（S 1 2 2）、第2の誤り検出符号情報として待避する（S 1 2 3）。そして、符号化画像データを暗号化する（S 1 2 4）。

【選択図】 図 1 2

特願 2003-015233

出願人履歴情報

識別番号

[000001007]

1. 変更年月日

1990年 8月30日

[変更理由]

新規登録

住 所

東京都大田区下丸子3丁目30番2号

氏 名

キヤノン株式会社